THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

MICHAEL EVERETTS,

on behalf of himself and all others similarly situated,

Plaintiff,

v.

PERSONAL TOUCH HOLDING CORP., a Delaware corporation,

Defendant.

Case No.: 21-2061

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Michael Everetts ("Plaintiff") brings this Class Action Complaint against Personal Touch Holding Corp. ("Defendant"), individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard sensitive information of patients and employees of Defendant or one of its subsidiaries and the dependents and spouses of such employees (collectively, "Class Members"), including, without limitation, first and last name, address, telephone number, date of birth, Social Security number (including those of dependents and spouses), financial information (including check copies, credit card numbers, and bank account information), driver's license number, passport number, birth certificate, background and credit report, demographic information, username and password used at Defendant, personal email address, fingerprint, retirement benefits information, welfare plan benefit number, and/or other information necessary for payroll (collectively, "personally identifiable information" or "PII") as well as medical treatment

information, insurance card, health plan benefit numbers, and/or medical record numbers (collectively, "protected health information" or "PHI").

2. According to its website, Defendant's "Personal-Touch Home Care" division "began operations in 1974, and since that time has grown into a national company with 25 locations in 7 states with over 15 locations certified by Medicare."[1] It "provide[s] skilled nursing, physical, occupational and speech therapy, medical social work and home health aides and companions" and "has developed specialty programs, including mental health, pediatrics, maternal/child, hospice, rehabilitation, early intervention and early childhood education, dialysis, infusion and others."[2]

3. On or before January 27, 2021, Defendant learned that "it experienced a cybersecurity attack on the private cloud hosted by its managed service providers" (the "Data Breach").[3]

4. At the time of the Data Breach, the compromised private cloud stored the PII and PHI of more than 750,000 current and former patients and employees, and dependents and spouses thereof, of Defendant or its direct and indirect subsidiaries.[4]

5. On March 25, 2021, Defendant notified the Office of the Maine Attorney General that the Data Breach was a ransomware attack and that it had begun notifying Plaintiff and Class Members of the Data Breach on March 24, 2021.

6. By obtaining, collecting, using, and deriving a benefit from the PII and PHI of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to

---

[1] *See* https://www.pthomecare.com/about (last visited Apr. 7, 2021).
[2] *Id.*
[3] Ex. 1 (*Notice of Security Breach* posted on the Personal-Touch Home Care website), *available at* https://www.pthomecare.com/protects (last visited Apr. 13, 2021).
[4] *Id.*

protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted PII and PHI exposed to "unauthorized activity" included names, Social Security numbers, dates of birth, and birth certificates.

7. The exposed PII and PHI of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

8. This PII and PHI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant waited approximately two months to report it to the states' Attorneys General and affected individuals. Defendant has also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiff and Class Members of that information.

9. As a result of this delayed response, Plaintiff and Class Members had no idea their PII and PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

10. Plaintiff brings this action on behalf of all persons whose PII and PHI was compromised as a result of Defendant's failure to: (i) adequately protect the PII and PHI of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII and PHI using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

11. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and certainly increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

12. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII and PHI of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII and PHI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

13. Plaintiff Michael Everetts ("Everetts") is a Citizen of Pennsylvania residing in Butler County, Pennsylvania. Mr. Everetts received Defendant's *Notice of Data Breach*, dated March 24, 2021, on or about that date.[5] The notice stated that Plaintiff's medical treatment

[5] Ex. 2.

information, insurance card and health plan benefit numbers, medical record numbers, first and last name, address, telephone numbers, date of birth, Social Security number, and financial information, including check copies, credit card numbers, and bank account information, may have been exposed.[6]

14. Defendant Personal Touch Holding Corp. is a corporation organized under the laws of Delaware, headquartered at 1985 Marcus Avenue, Lake Success, New York, with its principal place of business in Lake Success, New York.

15. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

16. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

17. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

18. The Eastern District of New York has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District

[6] *Id.*

and Defendant conduct substantial business in New York and this District through its headquarters, offices, parents, and affiliates.

19. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

20. Defendant, itself or through its subsidiaries, provides, among other things, home health care services in at least seven (7) states.

21. Plaintiff and Class Members entrusted Defendant with sensitive and confidential information, including first and last name, address, telephone number, date of birth, Social Security number (including those of dependents and spouses), financial information (including check copies, credit card numbers, and bank account information), driver's license number, passport number, birth certificate, background and credit report, demographic information, username and password used at Defendant, personal email address, fingerprint, retirement benefits information, welfare plan benefit number, and/or other information necessary for payroll as well as medical treatment information, insurance card, health plan benefit numbers, and/or medical record numbers, and other personal identifiable information, which include information that is static, does not change, and can be used to commit myriad financial crimes.

22. Plaintiff and Class Members, as current and former patients and employees and their dependents and spouses, relied on this sophisticated Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand

security to safeguard their PII and PHI.

23. Defendant had a duty to adopt reasonable measures to protect the PII and PHI of Plaintiff and Class Members from involuntary disclosure to third parties.

The Data Breach

24. On or about March 24, 2021, Defendant sent Plaintiff a *Notice of Security Breach*.[7] Defendant informed Plaintiff that:

> **WHAT HAPPENED:**
>
> On January 27, 2021, the Business Associate discovered it suffered a cybersecurity attack on its private cloud hosted by its managed service providers. We believe the cybersecurity attack occurred on or about January 20, 2021 through January 27, 2021. Upon discovery of the breach on January 27th, the Business Associate retained outside counsel and independent forensic experts to begin an investigation. While the investigation is ongoing, and we cannot confirm the extent to which your data was compromised, we are notifying you that the breach occurred, in our efforts to comply with the Health Information Portability and Accountability Act ("HIPAA") and with applicable state data breach notification laws.
>
> **WHAT INFORMATION WAS INVOLVED:**
>
> The Business Associate's private cloud stored business records of the Business Associate and its direct and indirect subsidiaries where your personally identifiable information and protected health information were contained. This information may include medical treatment information, insurance card and health plan benefit numbers, medical record numbers, first and last name, address, telephone numbers, date of birth, Social Security number, and financial information, including check copies, credit card numbers, and bank account information.
>
> **WHAT WE ARE DOING:**
>
> Upon discovering the breach, the Business Associate retained a team of third-party forensic technical experts to investigate the origins and scope of the breach. The Business Associate also notified the Federal Bureau of Investigations ("FBI") of the breach.

[7] Ex. 2.

> Pursuant to applicable law, we will be notifying the U.S. Department of Health and Human Services, Office of Civil Rights ("OCR"), which is responsible for enforcing the HIPAA Privacy and Security Rules. We will comply with OCR to meet requirements of the HIPAA Breach Notification Rule, which requires that patients be notified and will cooperate with regard to any further inquiry they may have. We will also be notifying state regulators as required by law.[8]

25. On or about March 25, 2021, Defendant notified various state Attorneys General, including Maine's Attorney General Frey, of the Data Breach. Defendant also provided the Attorneys General with "sample" notices of the Data Breach that reaffirm the information exposed in the Data Breach "may include medical treatment information, insurance card and health plan benefit numbers, medical record numbers, first and last name, address, telephone numbers, date of birth, Social Security number, and financial information, including check copies, credit card numbers, and bank account information.[9]

26. Defendant admitted in the *Notice of Data Breach*, the letters to the Attorneys General, and the "sample" notices of the Data Breach that unauthorized third persons accessed files that contained sensitive information about Plaintiff and Class Members, including names, Social Security numbers, dates of birth, and birth certificates.

27. In response to the Data Breach, Defendant claims that it "retained a team of third-party forensic technical experts to investigate the origins and scope of the breach. The Business Associate also notified the Federal Bureau of Investigations ("FBI") of the breach."[10] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information

[8] *Id.* at 1-2.
[9] Ex. 3.
[10] Exs. 2, 3.

remains protected.

28. The unencrypted PII and PHI of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII and PHI of Plaintiff and Class Members.

29. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for more than 750,000 individuals.

30. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[11]

31. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

[11] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Mar. 15, 2021).

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[12]

32. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on,

[12] *Id.* at 3-4.

as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[13]

33. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

[13] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Mar. 15, 2021).

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[14]

34. Given that Defendant was storing the PII and PHI of more than 750,000 individuals, collected since at least 2013, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

35. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII and PHI of more than 750,000 individuals, including Plaintiff and Class Members.

[14] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Mar. 15, 2021).

Defendant Acquires, Collects, and Stores the PII and PHI of Plaintiff and Class Members.

36. Defendant acquired, collected, and stored the PII and PHI of Plaintiff and Class Members at least from 2013 to 2020.

37. As a condition of treatment from or employment with Defendant or its subsidiary, Defendant or its subsidiary requires that patients and employees and their dependents and spouses entrust Defendant with highly confidential PII and PHI.

38. By obtaining, collecting, and storing the PII and PHI of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII and PHI from disclosure.

39. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and PHI and Preventing Breaches

40. Defendant could have prevented this Data Breach by properly securing and encrypting the private cloud containing the PII and PHI of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially decade-old data from former patients and employees and their dependents and spouses.

41. Defendant's negligence in safeguarding the PII and PHI of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

42. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiff and Class Members from being compromised.

43. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[16]

44. The ramifications of Defendant's failure to keep secure the PII and PHI of Plaintiff and Class Members are long lasting and severe. Once PII and PHI is stolen, particularly Social Security numbers and birth certificates, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

45. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[17] Experian reports that a stolen credit or debit

[15] 17 C.F.R. § 248.201 (2013).
[16] *Id*.
[17] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Dec. 30, 2020).

card number can sell for $5 to $110 on the dark web.[18] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[19]

46. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[20]

47. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

48. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the

---

[18] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Dec. 29, 2020).

[19] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 29, 2020).

[20] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Dec. 29, 2020).

new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[21]

49. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, name, and date of birth, and potentially government-issued ID number, mother's maiden name, birth certificate, and biometric information.

50. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[22]

51. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

52. The fraudulent activity resulting from the Data Breach may not come to light for years.

53. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data

[21] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Dec. 29, 2020).

[22] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Dec. 29, 2020).

> may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[23]

54. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiff and Class Members, including Social Security numbers, dates of birth, and birth certificates, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

55. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

56. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's private cloud, amounting to potentially hundreds of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

57. To date, Defendant has not offered Plaintiff and Class Members any identity theft detection or similar service, and instead merely suggested that Plaintiff and Class Members monitor their account statements, explanation(s) of benefits, and credit bureau reports. The failure to offer such service is highly unusual and reflects an indifference to the seriousness of the exposure, which includes Social Security numbers, dates of birth, and birth certificates. Defendant's paltry recommendation to self-monitor is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII and PHI at

[23] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Mar. 15, 2021).

issue here.

58. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiff and Class Members.

Plaintiff Michael Everetts' Experience

59. In or around 2013, Plaintiff Michael Everetts was a patient of Defendant or its subsidiary in or near Butler County, Pennsylvania. As a condition of treatment, Defendant or its subsidiary required that he provide his PII and PHI, including but not limited to his name, Social Security number, and date of birth.

60. Mr. Everetts received the Notice of Security Breach, dated March 24, 2021, on or about that date.

61. After the Data Breach, someone filed for pandemic unemployment assistance using Mr. Everetts' PII, without Mr. Everetts' knowledge or authorization.

62. As a result of the Data Breach notice, Mr. Everetts spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Security Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

63. Additionally, Mr. Everetts is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII and PHI over the internet or any other unsecured source.

64. Mr. Everetts stores any documents containing his PII and PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

65. Mr. Everetts suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that Mr. Everetts entrusted to Defendant for the purpose of his treatment, which was compromised in and as a result of the Data Breach.

66. Mr. Everetts suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

67. Mr. Everetts has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI, especially his Social Security number, in combination with his name and date of birth, being placed in the hands of unauthorized third parties and possibly criminals.

68. Mr. Everetts has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

69. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

70. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals whose PII or PHI was compromised in the breach that is the subject of the Notice of Data Breach that Defendant sent to Plaintiff on or around March 24, 2021 (the "Nationwide Class").

71. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of a separate subclass, defined as follows:

> All current and former patients of Defendant, or any of its direct or indirect subsidiaries, who had contracts related to PII or PHI that was compromised in the breach that is the subject of the Notice of Security Breach that Defendant sent to Plaintiff on or around March

24, 2021 (the "Patients Class").

72. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

73. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

74. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Defendant has identified hundreds of thousands of current and former patients and employees and their dependents and spouses whose PII and PHI may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records. Defendant advised Maine Attorney General Frey that the Data Breach affected 753,107 individuals.

75. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII and PHI of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

76. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other

Class Members because all had their PII and PHI compromised as a result of the Data Breach, due to Defendant's misfeasance.

77. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

78. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

79. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class

Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

80. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

81. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

82. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

83. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII and PHI of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

84. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

85. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual damages, statutory damages, nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

86. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 85.

87. As a condition of treatment from or employment with Defendant or its subsidiary, Defendant's current and former patients and employees were obligated to provide Defendant or its subsidiary with certain PII and PHI of themselves and their dependents and spouses, including names, Social Security numbers, dates of birth, and birth certificates.

88. Plaintiff and the Nationwide Class entrusted their PII and PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

89. Defendant has full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the PII and PHI were wrongfully disclosed.

90. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and PHI of Plaintiff and the Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm

occurred through the criminal acts of a third party.

91. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII and PHI of Plaintiff and the Nationwide Class in Defendant's possession was adequately secured and protected.

92. Defendant also had a duty to exercise appropriate clearinghouse practices to remove the PII and PHI of Plaintiff and Class Members it was no longer required to retain pursuant to regulations.

93. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiff and the Nationwide Class.

94. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Nationwide Class. That special relationship arose because Plaintiff and the Nationwide Class entrusted Defendant with their confidential PII and PHI, a necessary part of treatment from or employment with Defendant or its subsidiary.

95. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Nationwide Class.

96. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

97. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the

inherent risks in collecting and storing the PII and PHI of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that PII and PHI, and the necessity for encrypting PII and PHI stored on Defendant's systems.

98. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendant.

99. Plaintiff and the Nationwide Class had no ability to protect their PII and PHI that was in, and possibly remains in, Defendant's possession.

100. Defendant was in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

101. Defendant had and continues to have a duty to adequately disclose that the PII and PHI of Plaintiff and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties.

102. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiff and the Nationwide Class.

103. Defendant has admitted that the PII and PHI of Plaintiff and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

104. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Nationwide Class during the time the PII and PHI was within Defendant's possession or control.

105. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

106. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiff and the Nationwide Class in the face of increased risk of theft.

107. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of their PII and PHI.

108. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove the PII and PHI of Plaintiff and the Nationwide Class it was no longer required to retain pursuant to regulations.

109. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

110. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII and PHI of Plaintiff and the Nationwide Class would not have been compromised.

111. There is a close causal connection between Defendant's failure to implement

security measures to protect the PII and PHI of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII and PHI of Plaintiff and the Nationwide Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

112. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

113. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

114. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

115. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

116. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Nationwide Class.

117. As a direct and proximate result of Defendant's negligence and negligence *per se*,

Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

118. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

119. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Patients Class)

120. Plaintiff and the Patients Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 85.

121. Defendant required Plaintiff and the Patients Class to provide their personal information, including names, Social Security numbers, dates of birth, and other personal information, as a condition of their treatment. Defendant may have also required Plaintiff and the Patients Class to provide their medical treatment information, insurance cards, health plan benefit numbers, medical record numbers, addresses, telephone numbers, and financial information, including check copies, credit card numbers, and bank account information.

122. As a condition of their treatment with Defendant, Plaintiff and the Patients Class provided their personal and financial information. In so doing, Plaintiff and the Patients Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Patients Class if their data had been breached and compromised or stolen.

123. Plaintiff and the Patients Class fully performed their obligations under the implied contracts with Defendant.

124. Defendant breached the implied contracts it made with Plaintiff and the Patients Class by failing to safeguard and protect their personal and financial information and by failing to provide timely and accurate notice to them that personal and financial information was compromised as a result of the data breach.

125. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Patients Class have suffered (and will continue to suffer) ongoing,

imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Nationwide Class)

126. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 85.

127. Plaintiff and the Nationwide Class had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

128. Defendant owed a duty to Plaintiff and the Nationwide Class to keep their PII and PHI confidential.

129. Defendant failed to protect and released to unknown and unauthorized third parties the PII and PHI of Plaintiff and the Nationwide Class.

130. Defendant allowed unauthorized and unknown third parties access to and examination of the PII and PHI of Plaintiff and the Nationwide Class, by way of Defendant's failure to protect the PII and PHI.

131. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII and PHI of Plaintiff and the Nationwide Class is highly offensive to a reasonable

person.

132. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Nationwide Class disclosed their PII and PHI to Defendant or its subsidiary as part of employment or treatment with Defendant or its subsidiary, but privately with an intention that the PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

133. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Nationwide Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

134. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

135. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Nationwide Class.

136. As a proximate result of the above acts and omissions of Defendant, the PII and PHI of Plaintiff and the Nationwide Class was disclosed to third parties without authorization, causing Plaintiff and the Nationwide Class to suffer damages.

137. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Nationwide Class in that the PII and PHI maintained by Defendant can be viewed, distributed, and

used by unauthorized persons for years to come. Plaintiff and the Nationwide Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Nationwide Class.

COUNT IV
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Nationwide Class)

138. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 85.

139. At all times during Plaintiff's and the Nationwide Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Nationwide Class's PII and PHI that Plaintiff and the Nationwide Class provided to Defendant.

140. As alleged herein and above, Defendant's relationship with Plaintiff and the Nationwide Class was governed by terms and expectations that Plaintiff's and the Nationwide Class's PII and PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

141. Plaintiff and the Nationwide Class provided Plaintiff's and the Nationwide Class's PII and PHI to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII and PHI to be disseminated to any unauthorized third parties.

142. Plaintiff and the Nationwide Class also provided Plaintiff's and the Nationwide Class's PII and PHI to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII and PHI from unauthorized disclosure.

143. Defendant voluntarily received in confidence Plaintiff's and the Nationwide Class's PII and PHI with the understanding that PII and PHI would not be disclosed or disseminated to the public or any unauthorized third parties.

144. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff and the Nationwide Class's PII and PHI was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Nationwide Class's confidence, and without their express permission.

145. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Nationwide Class have suffered damages.

146. But for Defendant's disclosure of Plaintiff's and the Nationwide Class's PII and PHI in violation of the parties' understanding of confidence, their PII and PHI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and the Nationwide Class's PII and PHI as well as the resulting damages.

147. The injury and harm Plaintiff and the Nationwide Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Nationwide Class's PII and PHI. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Nationwide Class's PII and PHI was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Nationwide Class's PII and PHI.

148. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Nationwide Class, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with

effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

149. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the Patients Class and appointing Plaintiff and their Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive

and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII and PHI of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor

Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: April 15, 2021

Respectfully Submitted,

/s/ Amanda Peterson
Amanda Peterson (AP1797)
MORGAN & MORGAN
90 Broad Street, Suite 1011
New York, NY 10004
(212) 564-4568
apeterson@ForThePeople.com

John A. Yanchunis*
Ryan D. Maxey*
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

**pro hac vice* to be filed

Attorneys for Plaintiff and the Proposed Class